

© 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Citation:

Rathee, Geetanjali, Razi Iqbal, Chaker Abdelaziz Kerrache, and Houbing Song. "TrustNextGen: Security Aspects of Trustworthy Next Generation Industrial Internet of Things (IIoT)." IEEE Internet of Things Journal, 2024, 1–1. <https://doi.org/10.1109/JIOT.2024.3361801>.

DOI:

<https://doi.org/10.1109/JIOT.2024.3361801>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

TrustNextGen: Security Aspects of Trustworthy Next Generation Industrial Internet of Things (IIoT)

Geetanjali Rathee, Razi Iqbal, Chaker Abdelaziz Kerrache, Houbing Song

Abstract—With the expansion of Internet-of-Things (IoT), security of smart devices is becoming major or primary concern in today's era. The increasing demand of consumer electronics due its recent evolution, the personal information that is shared is becoming valuable. In addition, the next generation of Industrial Internet of Things (IIoT) devices include features such as low cost, automation, intelligence provision, reduced overhead, efficiency, and remote interactions while communicating or transmitting information among themselves. There are very few authors who have focused on next gen IIoT while improving the efficiency along with providing the security among devices in the network. Therefore, we have proposed a hybrid trusted model by integrating objective model and fuzzy evaluation matrix method to ensure a secure and efficient transmission method among devices in the network. The proposed mechanism is simulated and experimented over various parameters such as detection ratio and network-related performance and functional tests compared to state-of-art solutions.

Index Terms—Security, IIoT, trust identification, trusted methods, heterogeneous environment, next gen devices.

I. INTRODUCTION

Consumers are becoming increasingly educated and concerned about eco-friendly environmental safety devices, as the demand for such products continues to rise. The consumer electronics also referred to as home electronics are the electronics gadgets intended for everyday use for the consumers specifically for private homes [1]. It includes communications, entertainment and recreation that are meant for consumers usage. The market for consumer electronics equipment, intended for the everyday use of devices—whether static or automated, such as connected watches, home automation, smartphones, printers, refrigerators, etc.—is expanding with the growth of the Internet of Things (IoT). The security of smart devices is becoming a major or primary concern in today's era [2], [3]. The increasing demand of consumer electronics and IIoT due its recent evolution, the personal information that is shared is becoming valuable. The evolution and increasing demand of fast-growing consumer electronics and IIoT, the powerful devices such as smartphones, laptops, databases are introduced

with an exponential rate in the network. The advancement and improvement in IIoT devices in the network, the personal information of consumers also becoming rich and valuable. The huge demand of IIoT devices also brings security an privacy challenges in both active and passive manner [4], [5]. For example, the smart phones are also used to share live locations, money transfer using online banks, payment of goods, emailing, stock dealing, etc. this convenience also brings a huge lose or disaster if the smart phone is stolen or lost. In addition, the onetime purchase of any home appliance item such as washing machine, refrigerator may also get attacked by the intruder. The onetime usage of these purchased devices may also receive an alert message of paying some extra debt of using it [6], [7]. Though the device is already purchased by the owner at one time payment, however, the intruder may again send you the threaten email or alert message for paying some extra amount every time upon usage of these items. The general architecture of device's communication mechanism using four different layers of web internet-of-things is illustrated in Fig. 1. The data communication among devices along with identification of behaviour of each device is detected in share layer and findability layer. Further two layers such as compose layer and access and network layer are responsible of availability of resources and application specific data communication in the network [8].

A. Motivation

Security is a major challenge as well as ease of use for consumer electronics and IIoT devices. With the advent of smart home appliances, everyone has a connected device that puts the entire network into risk. In addition, the privacy is also a big concern that is increasingly vary about anything involving GDPR and cyberthreats in the networks [9], [10]. Therefore, to protect the private information or prevent the hacking of home appliances by any third party or intruder from misuse, some secure or trusted methods or user identification methods should be equipped with consumer devices. The security of personal information or home appliances can be guaranteed in variety of ways such as biometrics technology, IT security services etc [11], [12]. A number of privacy preservation techniques such as biometric or fingerprinting methods have been identified by several researchers/scientists, however, the security of home appliances usage after purchasing the entire product at the first place is still at its early stage. Further, the next gen consumer electronics in IIoT devices are the one which includes low cost, automation, intelligence provision, lesser overhead, efficient and remote interactions feature while transmitting or communicating the information among each other. The heterogeneous environment of intelligent devices may further create the issues

(Corresponding Authors: Chaker Abdelaziz Kerrache)

Geetanjali Rathee is with the Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi-110078, India. (e-mail: geetanjali.rathee123@gmail.com)

Razi Iqbal is with the Department of Computer Information Systems, University of Fraser Valley, Canada (e-mail: razi.iqbal@ieee.org)

Chaker Abdelaziz Kerrache is with the Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat, Algeria. (e-mail: ch.kerrache@lagh-univ.dz)

Houbing Song is with the Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, USA. (e-mail: songh@umbc.edu)

while transmitting the information in the network [13], [14]. In addition, the scalability of devices in an environment invites huge number of intruders who target is to degrade the network performance. There are very few authors who have focused on next generation IIoT while improving the efficiency along with providing the security among devices in the network. Therefore, the motivation of this paper, is to propose or present a secure and trustworthy mechanism for detecting the malicious behavior of devices involved while communicating with other devices in the network [15], [16].

B. Contribution

Though number of security schemes are present for efficient and effective communication in the network such as cryptographic, encryption schemes, third party schemes and so on. However, these mechanisms need extra storage space or computation and communication overheads while processing the information or to detect the legitimacy of a device. Trust is defined as a significant and efficient means of communication, ensuring a secure communication environment without incurring additional memory or key management costs. In the context of the next generation of Industrial Internet of Things (IIoT), where efficiency, robustness, and minimized storage and computations are deemed crucial factors, trust methods play a key role in providing security to devices by ensuring the mentioned factors. The other security methods such as cryptographic, algorithmic or encryption-based, all need significant computation, storage space, complexity, key management etc. that is further very crucial for ensuring a next gen secure consumer device. Therefore, the contribution of this paper is to propose a hybrid trusted model by integrating objective model [17] and fuzzy evaluation matrix [18] method to ensure secure and transparent communication mechanism among devices in the network. In addition, the proposed solution is further analyzed against several security metrics by comparing it with existing schemes.

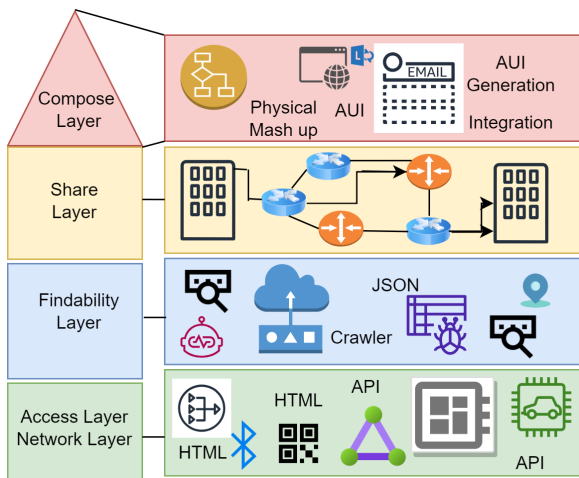


Fig. 1. General Architecture of Web-of-Things

The major contribution of the paper is further elaborated as:

- The fuzzy logic mechanism is used to analyze the trust of each communicating device by maintaining a distributed

hash table that may easily identify the varied number of devices in the network.

- In addition, the proposed approach uses objective trust model that provides the recommendation of legitimate devices to other neighboring devices in the network.
- The proposed scheme is further analyzed against various security measures such as delay, latency, data alteration, computation/communication cost etc.

The remaining organization of the paper is organized as follows: The number of papers presented by various authors are illustrated in section 2. A secure and transparent communication transmission by integrating the fuzzy evaluation matrix and integrating objective model is deliberated in section 3. In addition, section 4 discusses the verification and validation of proposed solution over existing schemes through various security metrics. Finally, section 5 concludes along with discussing the future scope of the paper.

II. LITERATURE SURVEY

This section illustrates the number of schemes and mechanisms proposed by various researchers/scientists in order to ensure an efficient and effective communication in the network. In order to understand the readability of the literature. The first subsection details the number of AI or intelligent based schemes proposed by several scientists. Further, various cryptographic and security schemes are discussed in second subsection of literature survey.

A. AI-based Security Schemes

Pal et al. [19] have designed a mixed method for collecting the data by combining semi-structured interviews and stated-choice experiments. The authors have used Exploratory Factor Analysis method for identifying the personal methods. In addition, the authors have used multinomial logit model for testing the proposed model in order to measure the security of network. The authors have experimented the results based on consumer electronics community perspectives. Khan et al. [20] have presented a framework to study by addressing the consumer electronics security from different five different perspectives such as gift, borrow, rent, retire and resale. The authors have presented the challenges and cybercriminals concerns while accessing the private information. The authors have also presented various challenges and privacy/security acts of violation. Further, the authors have also suggested the recommendations to preserve the privacy and security for IoT consumers. Kahleifeh et al. [6] have designed a secure and low-energy physical unclonable function using magnetic and adiabatic tunnel junctions for ensuring the security of consumer electronics. The authors have offered two different modes of communication operation depending upon tunnel junction orientation. The proposed methods are experimented over reliability by considering supply voltage, temperature, TMR variation.

Baghel and Prakash [21] have proposed a secure, non-invertible and alignment-free technique for generating a secure fingerprint template using discrete Fourier transform method. The authors have utilized the pair-polar structures in a 3D grid of minutiae. The proposed technique is analyzed over diversity, revocability, performance and security using four

TABLE I
LITERATURE SURVEY

Name of Author	Method/Scheme	Result Metrics	Limitation
Pal et al. [19]	Semi-structured interviews and stated-choice experiment	Used Exploratory Factor Analysis method for identifying the personal methods	No proposed mechanism
Khan et al. [20]	Framework to study and address the consumer electronics security	Presented various challenges and privacy/security acts of violation	Lot of computational delay is there
Kahleifeh [6]	Secure and low-energy physical unclonable function	Offered two modes of operation depending upon tunnel junction orientation.	System has complex computation
Baghel and Prakash [21]	Secure, non-invertible and alignment-free technique	Utilized the pair-polar structures in a 3D grid of minutiae	Leads to networking security threats
Das and Debnath [22]	Trusted computing model using various trust methods	proposed maximum possible factors trust model using NS3 simulation for executing the checks on trust values	Didn't propose any model
Fong and Westerink [23]	Comprehensive study on various technological challenges	Discussed three papers by covering the future aspects on affecting computing in IEEE transactions	There is no generalized solution to focus on challenges
Ding et al. [24]	novel framework to protect end users using deep learning technique	Compared the proposed mechanism against conventional approaches in terms of efficiency, detection performance and robustness	Real time transmission may be complex using proposed scheme

publicly available databases of fingerprints. the equal error rate metrics of proposed solution are compared with the state of art method for determining the effectiveness and robustness. Das and Debnath [22] have proposed a trusted computing model using various trust methods in different scenarios. The authors have proposed maximum possible factors trust model using NS3 simulation for executing the checks on trust values. The proposed mechanism is analyzed with accuracy and higher risk factors against conventional methods.

B. Cryptographic based security schemes

Fong and Westerink [23] have given a comprehensive study on various technological challenges affecting computing in consumer electronics. The authors have discussed three papers by covering the future aspects on affecting computing in IEEE transactions. The authors have targeted both consumer and business areas. Pero et al. [25] have illustrated the practical applications that are used for sharing the multimedia data among members of organizations. The authors have focused on securing on data exchange among members. In addition, the authors have focused on preventing the abusive information access without consent. Ding et al. [24] have proposed a novel framework to protect end users using deep learning technique via detecting attacks. The authors have compared the proposed mechanism against conventional approaches in terms of efficiency, detection performance and robustness.

C. Problem Statement

The number of security schemes have been projected by various researchers/scientists in order to provide the security to communicating devices. A number of privacy preservation techniques such as biometric or fingerprinting methods have been identified by several researchers/scientists, however, the security of home appliances usage after purchasing the entire product at the first place is still at its early stage. Further, the next gen consumer electronics devices are the one which includes low cost, automation, intelligence provision, lesser overhead, efficient and remote interactions feature while communicating

or transmitting the information among each other. There are very few authors who have focused on next gen consumer electronics while improving the efficiency along with providing the security among devices in the network.

III. PROPOSED MECHANISM

A. System Model

The depicted Figure 2 presents the trust-based IIoT architecture consisting of number of layers such as application layer, network layer, trusted layer and sensing layer. The application layer consists of decentralized, distributed, scalability and availability metrics that are further used by various applications such as military area, smart home, smart city and smart hospital. The transport layer is used to ensure the communication among devices through routers and availability of resources in the network. Further, trusted layer is embedded among transport and next gen layer in order to establish a transparent and secure communication while transmitting the information in the network. In order to provide a secure and trusted communication among IoT devices, the proposed mechanism uses hybrid trust model by integrating two trust models. Computational model and fuzzy evaluation matrix are the two trusted models for providing the secure communication among communicating devices. The fuzzy logic mechanism is used to analyze the trust of each communicating device by maintaining a distributed hash table that may easily identify the varied number of devices in the network. In addition, the proposed approach uses objective trust model that provides the recommendation of legitimate devices to other neighboring devices in the network. In addition, the detailed explanation of computational model and fuzzy evaluation matrix is listed in the further subsection.

B. Hybrid trust computation using fuzzy evaluation matrix and Objective trustworthiness

The computation of trust values of IoT devices are stored in Distributed Hash Table (DHT) structure that are available in chord, CAN and pastry. The DHT system are typically based on abstract key space where each device is completely

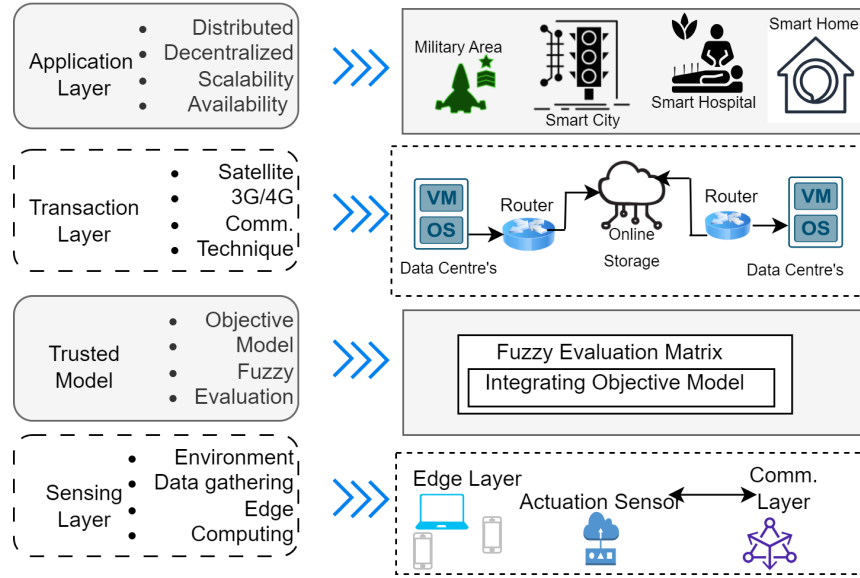


Fig. 2. Proposed Security Framework.

TABLE II
TABLE OF ABBREVIATION

Abbreviation	Description
D_a	Retrieve Information
MTD	Master Trust Device
D_i	i number of devices
D_{cxy}	Interaction of each alternatives
ET	Evidence of Trust
FM	Fuzzy Matrix
V_x	Evaluation matrix
α, β	Predefined threshold values
FM	Fuzzy evaluation matrix

responsible for their possibly generated set of keys. In order to store the transmitted file in the network, a key for the filename is computed using hash function where both the information and key are forwarded to the device which are responsible to hold that key. Let us take an example where D_a wants to retrieve the information by generating a key K and send it to DHT. The DHT will further hold the information along with the key and finally send the consent of retrieving the information to D_a . Now, in case of trust computation as depicted in Figure 2, where a device $d1$ queries the DHT for the information retrieval about route discovery namely $d4$, $d8$ and $d9$. In order to prevent from invention from malicious activities, the master trust device (MTD) are able to store and provide feedback of device trust in the network. Now, $D1$ will send the feedback about transaction to the MTD) which computes the new trust values of the devices involved in the previous communications. Then, through DHT, the MTD generates the key associated with information by storing the information for that key.

Whenever device d_i requires to know the recent trust value of another device d_j , it examines the DHT to recover it that is further computed as:

$$T_j = (1 - \alpha - \beta)D_j + \alpha MTD_j^{lon} + \beta MTD_j^{rec} \quad (1)$$

Where, α and β are defined as predefined threshold values

and MTD illustrates the master trust device (higher trust value devices) of long and recent devices.

Now, the trust of each device d_i is computed with the help of evaluation matrix method in order to further improve the accuracy of the complete system. The trust evaluation of a device not only depends upon its accuracy but affects or influences the neighboring devices or authorizers' accuracy. The evidence of trust is defined as $ET = et_1, et_2, \dots et_i$ and their evaluating level sets with trust values are defined as $ES = eg_1, eg_2, \dots eg_i$. After setting the ET and ES, fuzzy evaluation matrix will be designed as $FM = M_{xy}^{i*j}$, which is membership degree of ET_x to ES_y . Now, the weights are assigned to the devices by determining the entropy of x^{th} evidence as:

$$E_x = \frac{1}{\ln_j} \sum_{y=1}^j M_{xy} \ln(M_{xy}) + T_j \quad (8)$$

where $i \times j$ are the devices and $x \times y$ illustrates the evidences of devices at a time T .

$$M_{xy} \ln(M_{xy}) = 0, M_{xy} = 0 \quad (9)$$

The value of weight that is derived from ET_x is defined as:

$$\alpha = \frac{1 - ET_x}{n - \sum_{x=1}^i ET_x} + T_j \quad (10)$$

Hence, $\alpha_x \in [0,1]$ and $\sum_{x=1}^i \alpha_x = 1$

Further, the value of evidence level quantization is set as QL corresponding to the trust value evaluation level set i.e. TL as $QL = ql_1, ql_2, \dots ql_y$. The trust value of present device T_{Pr} is computed now computed as:

$$T_{Pr} = \sum_{x=1}^y QL_x \times V_x / \sum_{x=1}^y V_x + T_j \quad (11)$$

Algorithm 1 Trusted Algorithm**Step 1:** Compute queries for DHT:

$$T_j = (1 - \alpha - \beta)D_j + \alpha MT D_j^{lon} + \beta MT D_j^{rec} \quad (2)$$

Step 2: fuzzy evaluation matrix will be designed as $FM = (M_{xy}^{i*j})$:

$$E_x = \frac{1}{\ln_j} \sum_{y=1}^j M_{xy} \ln(M_{xy}) \quad (3)$$

$$M_{xy} \ln(M_{xy}) = 0, M_{xy} = 0 \quad (4)$$

Step 3: The separation measures are obtained for each alternate using Euclidean distance using:

The trust value of present device is computed as:

$$T_{PR} = \sum_{x=1}^y Q L_x \times V_x / \sum_{x=1}^y V_x + T_j \quad (5)$$

Step 4: The historical average trust of device is defined as:

$$T_{his} = \frac{1}{P} \sum_{R=1}^P T_{PR} \gamma(R) + T_j \quad (6)$$

 $Re[1, P]$, where $\gamma(R)$ is an depletion function to reduce the impact of previous trust evaluation on a device.**Step 5:** The final trust of device is computed as:

$$T_{final} = PR + \beta T_{his} \quad (7)$$

 $\alpha + \beta = 1$ depending on conditions.

Among, $V_x = V_1, V_2, \dots, V_y$ is the evaluation vector that is computed from the compound operation with respect to the analyzed evaluation matrix and weight vector. The historical average trust of device is defined as:

$$T_{his} = \frac{1}{P} \sum_{R=1}^P T_{PR} \gamma(R) + T_j \quad (12)$$

$Re[1, P]$, where $\gamma(R)$ is an depletion function to reduce the impact of earlier trust evaluation on a device. The final trust of device is computed as:

$$T_{final} = PR + \beta T_{his} + T_j \quad (13)$$

 $\alpha + \beta = 1$ depending on conditions.

Furthermore, in the proposed mechanism, the extended and recent recommendations are computed by taking into account the feedback received from all the remaining devices which are interacted with d_j as:

$$Rec_j^{extended} = \phi_{i=1}^y \phi_{l=1} E^{ex} B_{ij} W_{ij}^e f_{ij}^e / \phi_{i=1}^y \phi_{l=1} E^{ex} B_{ij} W_{ij}^e \quad (14)$$

Where, ϕ is defined as the constant threshold value and B_{ij} is benefit of device i to device j . In addition, the weight of each device is computed as W_{ij} to determine the recent and extended feedback reception.

$$Rec_j^{rec} = \phi_{i=1}^y \phi_{l=1} E^{rec} B_{ij} W_{ij}^e f_{ij}^e / \phi_{i=1}^y \phi_{l=1} E^{rec} B_{ij} W_{ij}^e \quad (15)$$

Further, in order to limit the malicious device involvement that may provide false feedback to the network, each feedback is weighted with device benefits (trustworthiness) by providing an additional factor. The benefits of device can be further measured as:

$$B_{ij} = \frac{(1 - \eta - \gamma)T_i + \eta(1 - F_{ij}) + \gamma(1 - I_j)}{1 + \log(N_{ij} + 1)} \quad (16)$$

Where, η, γ are the predefined threshold values and F_{ij} is the feedback of device j recommended by device i .

In this way, the devices with strong recommendations having high computation capabilities may have number of transactions among them. Algorithm 1 determines the trust computation model to identify the activeness and communicating behaviour of the IoT devices.

IV. PERFORMANCE ANALYSIS

A. Evaluation Criteria

The proposed mechanism is tested and verified using network simulator and was implemented in a synthesized dataset. The experimental tests were passed by verifying the proposed approach in three different ways such as: performance test, functional test and security test. The simulation area is chosen as $800m \times 800m$ having approximate 100 number of communicating devices. The identification of legitimate and altered devices are selected by including the malevolent devices and then analyze the performance of proposed mechanism. In addition, the trust values are distributed among $[0 - 1]$ that may be further increased or decreased depending upon its communicating behavior. The transmission power while sending/receiving the information is selected between $[15 - 35]$ dBm. The resources and receiving power of the network is decided as 10 dBm and 10^3 CPU cycles/unit time respectively. The definition of various test such as performance test, functional test and security test that are considered while identifying the validity of the proposed mechanism is discussed as follows:

- Performance test: The performance test is measured against eavesdropping, accuracy, delay of the information.
- Functional test: Authentication and confidentiality are considered as two functional tests criteria's for verifying the legitimacy of devices by presenting their computational and communicational analysis.
- Security test: It is measured over forgery, masquerade and data alteration scenarios.

B. Baseline Methods

The proposed solution is simulated over two existing methods as baseline scheme 1 and baseline scheme 2 for validating and

verifying the results. Das and Debnath [22] considering as baseline scheme 1 for this paper have proposed a trusted computing model using various trust methods in different scenarios. The authors have proposed maximum possible factors trust model using NS3 simulation for executing the checks on trust values. The proposed mechanism is analyzed with accuracy and higher risk factors against conventional method. In addition, Khan et al. [20] considering as baseline scheme 2 have presented a framework to study and addressed the consumer electronics IIoT challenges in security from five different perspectives such as gift, borrow, rent, retire and resale. The authors have presented the challenges and cybercriminals concerns while accessing the private information. The authors have also presented various challenges and privacy/security acts of violation. Further, the authors have also suggested the recommendations to preserve the privacy and security for IoT consumers. The proposed solution is simulated against these two mechanisms in terms of several security measure such as performance test, security test and functional test. Furthermore, the simulation behaviour and complete set up environment of proposed scheme is mentioned in Table III.

TABLE III
SIMULATION METRICS OF PROPOSED FRAMEWORK

Metrics	Terms
Simulation area	800 m \times 800 m
Number of communicating devices	100
% of malevolent devices	[5, 15]%
Computed Trust Results	[0, 1]
Transmission power	[15, 35] dBm
Receiver power	10 dBm
Resources	10^3 CPU cycle/unit time

C. Comparison and Discussion of Results

- **Latency:** It is defined as the amount of time required to transmit the information among source and destination through intermediate devices that are already compromised by the intruders.
- **Delay:** It is illustrated as the time needed to verify or prove the legitimacy of communicating devices while identifying its behavior by applying any security technique. In proposed work, we have used hybrid combination of fuzzy evaluation matrix and objective trustworthiness approaches to measure the legitimacy of a device.
- **Data alteration:** It is termed as the number of packets that are transmitted by the source device in the network and can be successfully compromised or altered by the intermediate entities in the network.
- **Masquerade:** It is the type of threat where information transmitting is maliciously or deliberately delayed by consuming the network resources by the intruders in the network.

In the context of the next generation of Industrial Internet of Things (IIoT), where efficiency, robustness, and minimized storage and computations are the major factors in order to establish the trust in the network. The proposed mechanism is analyzed against latency, data alteration, accuracy, computation and communication cost in order to prove the crucial factors. The efficiency and storage of records while transmitting the

information using proposed mechanism out-performed as compare to existing approaches because of less delay and critical analysis of device's identification during the data transmission. The involvement of trusted devices that are analyzed during the transmission process reduces the efforts of excessive storage and key management along with reduced the latency in order to improve the efficiency of the system. In addition, robustness of the system is analyzed through data alteration mechanism where how the system may behave and identify the malicious devices in the network with reduced delay and latency improves the overall performance of the network. Further, the computation is analyzed using computational and communication steps required to identify the trusted behaviour of a device in the network.

Figure 3 presents the latency of both existing and proposed mechanism concerning the number of devices. The results show the total latency of proposed mechanism that is much efficient as compare to existing schemes because of hybrid trust models for ensuring the significant accuracy. The improved accuracy of measuring the legitimacy of a device which may decreases the latency of communicating the information in the system.

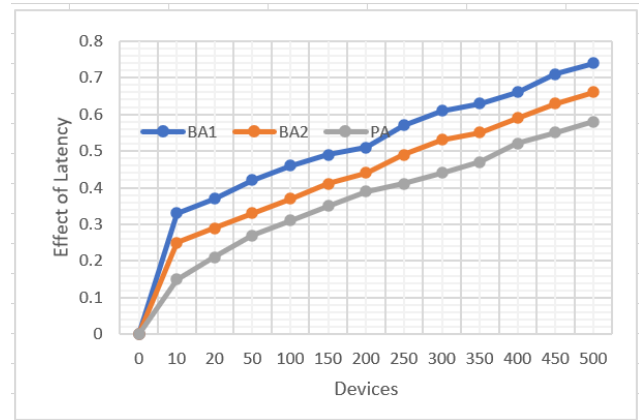


Fig. 3. Latency effect

Figure 4 illustrates the amount of delay required to identify or verify the legitimacy of proposed approach as compare to existing mechanisms. The proposed scheme takes less delay while addressing the malicious behavior of each communicating nodes. The reason is that the proposed approach needs less delay because of continuous surveillance and computation of each device trust values using fuzzy evaluation scheme. The integrated scheme further strengthens the possibility of legitimate device with no delay in response of any other device's query.

Data alteration is considered as the number of information that are successfully altered by the intruders while transmitting in the system. The depicted Figure 5 presents the hybrid combination of trust values in proposed approach maximizes the possibility of legitimate devices involvement during the message transmission process. The data alteration rate in case of proposed approach is very less in comparison of existing schemes.

Masquerade attack is termed where data communication is maliciously delayed by the intermediate devices in the system as illustrated in Figure 6. The malicious behavior of device altered by the intruder may drastically affect the overall performance of

TABLE IV
ANALYSIS OF MEASURING AGAINST VARIOUS PARAMETERS USING AN EMPIRICAL STUDY

Features	Resiliency	Efficiency	Anonymity	Persistency	Decentralized
Eavesdropping		✓		✓	✓
Reliability	✓		✓		
Access Control	✓		✓		
Trust Failure		✓	✓		
Data Honesty		✓			
Trusted Third Party	✓				✓

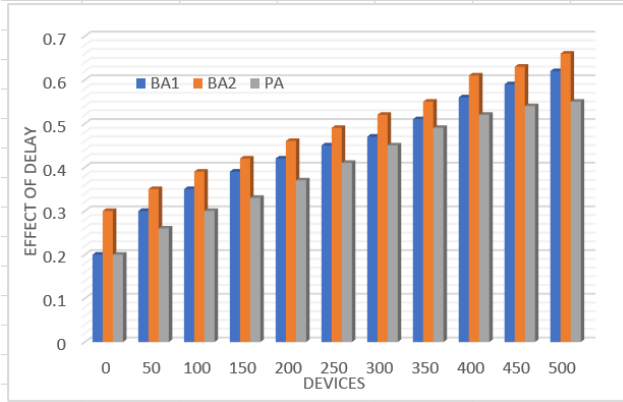


Fig. 4. End-to-end Delay

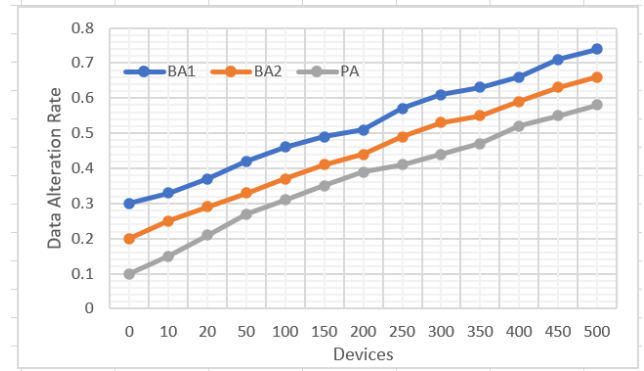


Fig. 6. Masquerade Attack

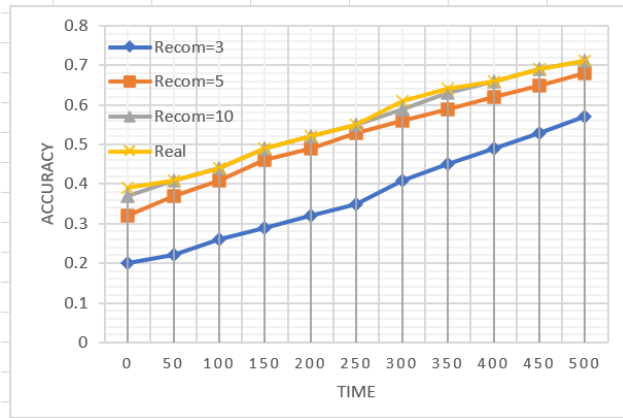


Fig. 5. Data Alteration

the network. The possibility of malicious devices involvement while transmitting the information in case of proposed approach is very less as compare to existing mechanism because of hybrid trust computation of each device in the system.

D. Empirical Study

Further, the security measuring analysis of the proposed and baseline approaches analysis through an empirical study is depicted in Table IV consisting of various factors such as reliability, accessibility, eavesdropping, transaction failure etc. In addition, the computational and communication cost of functional and performance test are depicted in Table V and Table VI corresponding to proposed and baseline mechanisms. Furthermore, the proposed mechanism can be easily measured against Rate-of-Reliability (RoR) that defines the reliability of the system against any cause of failure. The validity of proposed

scheme is analyzed against delay, information alteration and computation/communication costs that shows the reliability of system in the network. The RoR is better in terms of cost, delay, alteration over maintaining the efficiency, resiliency, anonymity, decentralized and persistence of environment while transmitting the information in the network.

TABLE V
COST AND TIME COMPARISON

Scheme	Communication	Comm. Cost	Comm. Time
BS1	V2V	$6T_h + T_{AE}$	5.61
BS2	V2V	$10T_h$	0.95
PA	V	T_s	17.2

TABLE VI
COMPUTATIONAL COST

Scheme	Communication	Comm. Cost	Comm. Time
BS1	V2V	$14L_s$	2.17
BS2	V2V	$5L_h + 2L_t$	7.12
PA	V	$10L_s$	3.15

Finally, the accuracy of the proposed and existing algorithms is presented in Table VII and their corresponding analysis is presented in Figure 7.

TABLE VII
ACCURACY

Algorithm	Accuracy
BS1	98.87
BS2	99.18
PA	99.54

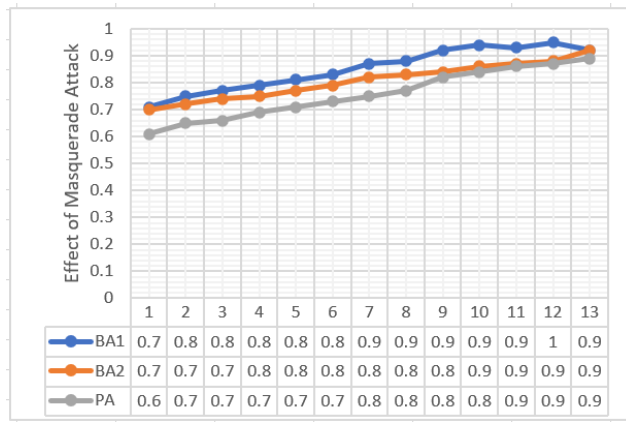


Fig. 7. Accuracy

E. Summary

Though various researchers and scientists have proposed number of security schemes and mechanisms in their previous studies. However, the existing approaches leads to key management, storage, accuracy and computation/communication costs. The proposed approach integrates objective and fuzzy evaluation matrix that are the examples of trusted schemes. The trust-based approaches require less time, more accuracy and reduced communication and computation overhead. The proposed mechanism is validated which shows the out-performance over three scenarios along with accuracy, cost and other security metrics against existing schemes. The fuzzy logic mechanism is used to analyze the trust of each communicating device by maintaining a distributed hash table that may easily identify the varied number of devices in the network. In addition, the proposed approach uses objective trust model that provides the recommendation of legitimate devices to other neighboring devices in the network. Further, the proposed approach is analyzed over an empirical study that depicts various security features along with several brute force methods.

V. CONCLUSION

Trust is defined as one of the significant and efficient way of communicating and ensuring a secure communication environment. By considering a next generation consumer electronics in IIoT where efficiency, robustness, less storage and computations are considered as major factors. The proposed solution is simulated against various test levels such as functional test, performance test and security test. The out-performance of proposed solution in comparison of existing mechanisms over all the approach are because of hybrid integration of objective and fuzzy evaluation matrix methods for short- and long-term recommendation of trust values to the communicating devices. The proposed mechanism efficiently ensures a secure communication process in the network. The optimization and energy consumption approaches that are further required to improve overall quality of the network may be considered in the future scope of this paper.

ACKNOWLEDGMENTS

This work has been funded by R&D project SERB-SURE SUR/2022/001051.

REFERENCES

- [1] J. Li, X. Zeng, and A. Stevels, "Ecodesign in consumer electronics: Past, present, and future," *Critical Reviews in Environmental Science and Technology*, vol. 45, no. 8, pp. 840–860, 2015.
- [2] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Zörjen, and B. Stiller, "Landscape of iot security," *Computer Science Review*, vol. 44, p. 100467, 2022.
- [3] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "{IoTPOT}: Analysing the rise of {IoT} compromises," in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, 2015.
- [4] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to iot security," *IoT security: advances in authentication*, pp. 27–64, 2020.
- [5] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.
- [6] Z. Kahlefeh, H. Thapliyal, and S. M. Alam, "Adiabatic/mjt-based physically unclonable function for consumer electronics security," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 1–8, 2022.
- [7] Y. Djenouri, A. Yazidi, G. Srivastava, and J. C.-W. Lin, "Blockchain: Applications, challenges, and opportunities in consumer electronics," *IEEE Consumer Electronics Magazine*, 2023.
- [8] B. Nour, M. Pourzandi, and M. Debbabi, "A survey on threat hunting in enterprise networks," *IEEE Communications Surveys Tutorials*, vol. 25, no. 4, pp. 2299–2324, 2023.
- [9] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.
- [10] A. Boulemtafes, A. Derhab, and Y. Challal, "A review of privacy-preserving techniques for deep learning," *Neurocomputing*, vol. 384, pp. 21–45, 2020.
- [11] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Next generation backscatter communication: systems, techniques, and applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–11, 2019.
- [12] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE access*, vol. 5, pp. 16 693–16 746, 2017.
- [13] J. Wang, M. Wang, Z. Zhang, and H. Zhu, "Toward a trust evaluation framework against malicious behaviors of industrial iot," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21 260–21 277, 2022.
- [14] Z. Zhou, Y. Tian, J. Xiong, J. Ma, and C. Peng, "Blockchain-enabled secure and trusted federated data sharing in iiot," *IEEE Transactions on Industrial Informatics*, 2022.
- [15] A. A. Fröhlich, L. P. Horstmann, and J. L. C. Hoffmann, "A secure iiot gateway architecture based on trusted execution environments," *Journal of Network and Systems Management*, vol. 31, no. 2, p. 32, 2023.
- [16] M. J. Gill, D. J. Gill, and T. J. Roulet, "Constructing trustworthy historical narratives: Criteria, principles and techniques," *British Journal of Management*, vol. 29, no. 1, pp. 191–205, 2018.
- [17] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on knowledge and data engineering*, vol. 26, no. 5, pp. 1253–1266, 2013.
- [18] J. Wang, H. Wang, H. Zhang, and N. Cao, "Trust and attribute-based dynamic access control model for internet of things," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, 2017, pp. 342–345.
- [19] D. Pal, V. Vanijja, X. Zhang, and H. Thapliyal, "Exploring the antecedents of consumer electronics iot devices purchase decision: a mixed methods study," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 4, pp. 305–318, 2021.
- [20] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Communal acts of iot consumers: A potential threat to security and privacy," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 1, pp. 64–72, 2018.
- [21] V. S. Baghel and S. Prakash, "Generation of secure fingerprint template using dft for consumer electronics devices," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 2, pp. 118–127, 2022.
- [22] P. Das and S. Debnath, "A trust computing model for future generation networks," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2020, pp. 1–4.
- [23] B. Fong and J. Westerink, "Affective computing in consumer electronics," *IEEE transactions on affective computing*, vol. 3, no. 2, pp. 129–131, 2012.
- [24] F. Ding, G. Zhu, M. Alazab, X. Li, and K. Yu, "Deep-learning-empowered digital forensics for edge consumer electronics in 5g hetnets," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 42–50, 2020.

- [25] C. Pero, L. Cimmino, L. Maiuri, F. Picano, and A. Castiglione, "Achieving a lawfully-secure audio recording framework using consumer electronics," in *2023 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2023, pp. 1–3.